North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Mailbox explodes at Bismarck residence. A white plastic mailbox exploded July 14, Bismarck, North Dakota police said. A firework or possibly an artillery shell damaged the mailbox, worth about $20, at the 3000 block of Homestead Drive. According to the police report, the owner said he saw a red, early 1990s GM car drive slowly by his house after he heard the explosion. He said the driver was a male in his late teens. No one has been arrested in connection with the explosion. Source: http://www.bismarcktribune.com/news/local/crime-and-courts/article_6aebdd0a-9032-11df-bfdc-001cc4c002e0.html

James River dam releases reduced. The Army Corps of Engineers said releases from southeast North Dakota dams on the James River have been cut after heavy rain downstream. Corps officials in Omaha, Nebraska, said combined releases from the Jamestown and Pipestem dams have been cut from 900 cubic feet per second (cfs) to 650 cfs. Water is being released from the reservoirs because both have risen into the flood pool after wet weather this year. The Corps said that with normal rainfall and inflows, the Jamestown flood pool should be evacuated by late July, and Pipestem evacuated by late August. Source: http://www.ksfy.com/Global/story.asp?S=12810813

Anthrax case confirmed in North Dakota livestock. North Dakota's top animal health official is urging livestock producers in areas with a history of anthrax to take action to protect their animals from the disease. "A single case of anthrax has just been confirmed in northwestern Dickey County, where the disease has been reported in the past," the state veterinarian said. "With weather conditions almost ideal for anthrax, producers need to make sure their animals are up to date on vaccinations." The Veterinary Diagnostic Laboratory at North Dakota State University confirmed the diagnosis of anthrax in a beef bull July 13. It is the second case of anthrax recorded in the state this year. Last May, an animal died from anthrax in Sioux County, the first confirmed case in that area in many years. An effective anthrax vaccine is readily available, but it takes about a week to establish immunity and must be followed with annual boosters. Source: http://www.agweek.com/event/article/id/16743/

Regional

(Montana) **Large wildfire burning near Canyon Ferry Reservoir.** A large wildfire is burning near Canyon Ferry Reservoir east of Helena, Montana, and several homes in the area have been evacuated. The York Fire, which was reported at about 6 p.m. July 16, started on the Ward Ranch below the dam on the north side of the reservoir. A Helena National Forest spokeswoman said about 360 acres had burned by 7:30 p.m., and residents were being evacuated from homes along Jimtown and Ward roads toward Canyon Ferry. About 25 people have been evacuated from the Riverside Campground. The sheriff saod about 150 firefighters will work through the night to contain the fire. Four helicopters, as well as engines from the U.S. Forest Service, the Montana Department of Natural Resources and Conservation, and from several volunteer fire departments, also are being used. The spokeswoman said the blaze is not threatening the dam. Source:

http://www.greatfallstribune.com/article/20100716/NEWS01/100716013/Large+wildfire+burning+near+Canyon+Ferry+Reservoir

National

(Oregon) **'Unabomber' hoax shuts down traffic near LO gas station.** The Lake Oswego, Oregon Police Department investigated a report of a suspicious device at a local gas station July 13. The incident occurred about 4:30 p.m. at the Chevron Service Station located at Boones Ferry and Reese roads. A station attendant reported having a conversation with a man. "[The suspect] arrived to get gas and was filling up his pickup," police said. "At one point [he] placed a silver metal briefcase on top of the gas pump. After getting gas and starting to leave it is reported [he] stated to the attendant, 'I'm the Unabomber' while driving off and pointed towards the briefcase left behind." The suspect left the scene and the attendant picked up the briefcase and carried it into the store and then called police. "As is standard procedure with suspicious devices, especially those left at service stations containing thousands of gallons of fuel, the intersection was shut down and members of the Portland Police Bureau Bomb Squad were called to evaluate the device," police said. "Traffic was rerouted in order to safeguard the public while the device was checked out. The briefcase was found to contain nothing more than papers." The suspect later returned to the service station and was detained. He was cited on suspicion of second-degree disorderly conduct. Source: http://www.portlandtribune.com/news/story.php?story_id=127907713839025000

International

MP warns telecoms exposed to infiltration. The current state of the telecommunications sector in Lebanon exposes it to security infiltration, the head of the Media and Telecommunications Parliamentary committee said July 14. He explained that damage was sustained by the telecommunications sector when a former employee in the field provided Israeli intelligence with sensitive information enabling it to monitor the entire telecommunications network. The technician in state-run Alfa telecommunications firm was arrested in June by Lebanese authorities on charges of providing the Israelis with crucial data. During the investigation, the detainee confessed that he had been collaborating with Israeli authorities since 1996. "There are responsibilities that should be shouldered by [telecom] firms, and a vital role for the state to play in protecting this sector by practical measures," the head of the Media and Telecommunications Parliamentary committee said. The technician was charged July 13 with spying for Israel. Another Israeli spy was sentenced to death at the same day. Source: http://www.istockanalyst.com/article/viewiStockNews/articleid/4309089

(Puerto Rico) **Dengue epidemic threatens Caribbean, kills dozens.** Mosquito-borne dengue fever is reaching epidemic stages across the Caribbean, with dozens of deaths reported and health authorities concerned it could get much worse as the rainy season advances. The increase in cases is being blamed on warm weather and an unusually early rainy season, which has produced an explosion of mosquitoes. Health officials said the flood of cases is straining the region's hospitals. Hospitals in Trinidad are running out of beds, and Puerto Rico is facing what officials say could be its worst dengue outbreak in more than a decade. At least five people have died in the U.S. Caribbean territory, and another 6,300 suspected cases have been reported as of mid-July. There are four types of dengue, and all cause fever, headaches and extreme joint and muscle pain. Most victims recover within a week, and while they become immune to the specific type of dengue they caught, they are

still vulnerable to other types. Health officials fear the virus could also gain a foothold in the United States. While test results for a suspected dengue case in the Miami area came back negative this week, a recent study found five percent of Key West residents show evidence they have been exposed to the virus. Source: http://www.google.com/hostednews/ap/article/ALeqM5jMbeYpmSDHNz0b1R9BLHDyNIiwrgD9H13GBO0

4 arrested in S. Africa with low-radiation device. Four South Africans were arrested in the capital Pretoria for trying to sell a low-radiation industrial nuclear device, police said July 10, insisting the incident had no link the World Cup. "Four people were arrested, all South Africans, they were trying to exchange or sell this particular device," said a spokesman for the elite investigative unit known as the Hawks. The suspects were arrested Friday at a garage in a sting operation that included a police helicopter, he said. The origin of the device is still under investigation. Pretoria is a major producer of nuclear medicine used to treat some cancers. "As a device, it's harmless unless someone opens it and even then, you would have to sit on it for hours to be at risk," the spokesman said. "It is out of circulation, people were arrested, investigations are ongoing, so there is no need to be afraid," he added. The four men will appear in court July 12. Police are still investigating if the men had links to any international network. The spokesman declined to comment on whether the device could be used to make a "dirty bomb." Source: http://www.khaleejtimes.com/DisplayArticle08.asp?xfile=data/international/2010/July/international_July368.xml&section=international

Banking and Finance Industry

(Tennessee) **Bomb threats force evacuations at Home Depot, Bank of America.** Telephoned bomb threats July 16 forced the evacuation of two businesses near Northgate Mall in Chattanooga, Tennessee, a Chattanooga Police Department spokeswoman said. Both the Home Depot at 1944 Northpoint Blvd. and the Bank of America branch at 1945 Northpoint Blvd. were searched and no explosive devices found. Workers and customers returned to the buildings after about 45 minutes. Police are working to locate the caller or callers. Source: http://www.timesfreepress.com/news/2010/jul/16/chattanooga-bomb-threats-force-evacuations-home-de/

(Illinois) **Police: Man drove car bomb into a bank.** A man is in custody on charges of felony arson after allegedly driving a car bomb into a Lockport, Illinois bank July 16. The 48-year-old suspect, of Blue Island, Illinois, was arrested after witnesses at the scene identified him, the Lockport Police Department said. He drove his car into the front entrance of a PNC bank, police said. The car exploded as the suspect walked away, police said, adding that he used the same material found in fireworks. No injuries were reported because the bank was closed and unoccupied, authorities said. The suspect is being held on charges of felony arson and felony criminal damage to property with an incendiary device. His motive is unknown, according to police. Source: http://www.cnn.com/2010/CRIME/07/17/illinois.carbomb/

Consumers warned about Amazon.com scam. The millions of consumers who use Amazon.com to purchase everything from books to cookware have to be careful about a new phishing scheme. The Better Business Bureau (BBB) said it has received reports of e-mails, appearing to come from

Amazon.com customer service, with the subject line "Thank you for your order." The message has the Amazon.com logo and looks legitimate in other ways, at least on the surface. The e-mail lists an order number, total price, and a link to view the order. Someone receiving the message who had not ordered anything might click the link to see what he has mistakenly been charged for. Someone who had actually ordered something from Amazon might click the link because the price and item description is wrong. Anyone who clicks on the link would be sent to a fake site where an attempt would be made to steal her personal information. Source: http://www.consumeraffairs.com/news04/2010/07/bbb_amazoncom_scam.html

Outage snarls processing of food stamps. System outages on July 15 and 16 may have crimped the shopping plans of some recipients of food stamps on the East Coast. The outages affected people in as many as 10 states that are served by J.P. Morgan, including Connecticut, New York and New Jersey, said a communications director for the Connecticut Department of Social Services. The outage is being blamed on a connectivity issue between J.P. Morgan, and one of its processors. There is a manual voucher process available to all retailers who participate in the Supplemental Nutrition Assistance Program (SNAP) that is being used until the system is back online. The back-up process requires a form to be completed by the retailer, a phone call to be made for an authorization number, and a signature from the client confirming the sale. Retailers would then clear the voucher within 15 days to receive payment. With this process, clients can have full access to their SNAP benefits. Source: http://www.ctpost.com/local/article/Outage-snarls-processing-of-food-stamps-580454.php

Bank of America phishing scam. ScanSafe reports a new phishing scam on the Bank of America Web site where the link provided for signing in to online banking points to a gramsbbq.org/bain (a Web site belonging to barbecue establishment in California), which in turn automatically redirects tusers to a phishing page hosted on chasingarcadia.com - another legitimate, but compromised, site belonging to a Canadian band. The use of compromised sites for redirecting and hosting phishing pages is a technique successfully used by many scammers, since it allows the e-mails to bypass reputation filters and community-based trust reporting. Experts note that the scams are easily detected — if one knows what to look for. Positioning the cursor on the link reveals that the domain it points to is not the official domain of the bank. And if one follow the link, the URL in the address bar will tell you the same. Source: http://www.net-security.org/secworld.php?id=9592

(Missouri) **'Phishing' scam targeted local bank.** An identity "phishing" scam discovered July 13 has targeted Mid America Bank customers who use mobile/wireless service provided by AT&T. The president of the Wardsville, Missouri-based bank said the bank's phone lines were inundated with calls from customers and non-customers. They had received calls stating their debit/credit cards had been inactivated. The caller asked them to press "1" to reactivate the card, then attempted to get their personal account information. Two customers notified Mid-America that they provided information about their debit cards. The bank "hotcarded" the cards to freeze any account activity, the bank's IT systems administrator said. No funds have been illegally withdrawn through the scam. If customers report that they gave out their banking information and money is withdrawn from an account, the bank has protection through its credit card company to reimburse the losses. Source: http://newstribune.com/articles/2010/07/15/news_local/nt169local12phishing10.txt

(Missouri) **Phishing scam targets local bank customers.** Scammers targeted Mid-Missouri bank customers July 13. Several viewers contacted the KRCG newsroom to report an automated call received on their cell phones. The message tells the recipient their Mid-America Bank debit card has been deactivated, and to enter the card number to continue. The Mid-America Bank confirmed the calls are not legitimate. The message is part of a phishing scam intended to trick recipients into giving up credit card numbers for fraudulent use. The calls targeted AT&T mobile customers in Mid-Missouri, whether or not they are customers of Mid-America Bank. Mid-America Bank said their customers' information has not been compromised. Source: http://www.connectmidmissouri.com/news/story.aspx?id=482376

ZeuS Trojan attempts to exploit MasterCard, Visa security programs. The notorious ZeuS banking Trojan is showing off a new trick: Popping up on infected computers with a fake enrollment screen for the "Verified By Visa" or "MasterCard SecureCode Security" programs. The real and legitimate Visa and MasterCard card-fraud prevention programs have cardholders use a password when making card-based purchases online as an additional means of security. The Zeus Trojan, with its ever-growing capability to steal financial information and execute unauthorized funds transfers, has recently been seen attacking banking customers on infected machines by displaying a fake "Verified by Visa" enrollment screen, or its MasterCard counterpart SecureCode, trying to lure victims into a fraudulent online enrollment action that would end up giving criminals sensitive financial data. "When you log into your bank, it says you have to enroll in Verified by Visa, that it is regulated now and you have to do it," explains the CEO at Trusteer, a security firm that makes software specifically designed for use by banks and their customers to deter malware of this kind. The remotely controlled ZeuS botnet, used by criminal organizations, infects PCs, waits for the victim to log onto a list of targeted banks or financial institutions, and uses various ruses to steal credentials or execute unauthorized funds transfers. This newer attack with utterly fake Verified by Visa and MasterCard SecureCode is designed to trick banking customers into giving over their personal identification numbers, Social Security numbers, credit- and debit-card numbers with expiration dates, and more, the CEO said. "We are investigating ZeuS so we encounter new variants." Source: http://www.networkworld.com/news/2010/071310-zues-mastercard.html?hpg1=bn

Visa recommends weighing card readers to detect tampering. According to reports, Visa has revoked security approval for two Ingenico card readers (3070MP01 and i3070EP01), apparently in response to successful modification by skimmers. By introducing additional electronic components, the skimmers were able to store and later retrieve credit card details and PIN numbers. The compromised PIN entry devices (PEDs) are reported to be old models primarily used in the United states. Visa has also published a list of other PEDs which do not meet the PCI standard and are frequent targets of skimming attacks. Although this type of attack is not a new phenomenon, Visa's response is, according to industry experts, surprising. The report states that this is the first time a specific vendor has been named and the first time Visa has admitted that a PCI-compliant retailer has fallen victim to an attack. The specifications contained in the Payment Card Industry Data Security Standard (PCI DSS) are intended to prevent attacks on computers and credit card systems. Although the number of compromised PEDs appears to be on the rise, an internal Visa memo states that approval of the devices was revoked as a purely precautionary measure. Source: http://www.h-online.com/security/news/item/Visa-recommends-weighing-card-readers-to-detect-tampering-1035293.html

(Louisiana) **Telephone debit card scam rampant in St. Charles Parish.** The sheriff of St. Charles Parish, Louisiana warned residents July 9 about a telephone scam asking people for their debit card numbers. Residents throughout the parish have reported receiving automated telephone calls, purportedly from the First National Bank of St. Charles that show a local number on caller ID. The recorded message advises that the resident's debit card has been canceled and asks the resident to punch in his or her debit card number to have it reinstated. Armed with such information, thieves have been able to steal money. The sheriff said the calls are originating from a Web-based system and are virtually untraceable. He has verified that several residents have become victims of the scam. A flurry of calls disrupted the switchboard at St. Charles Parish Hospital July 6. Source: http://www.nola.com/crime/index.ssf/2010/07/telephone_debit_card_scam_ramp.html

(Maryland) **Police uncover fake credit card operation.** Anne Arundel County, Maryland police on foot patrol recently discovered a phony credit-card operation while investigating an illegally parked sports car outside a convenience store in Annapolis. Three Brooklyn, New York men were arrested at the scene and charged with creating more than 70 faux cards. Detectives now are piecing together how the fake plastic was made and whether identities were stolen in the process, said a county police spokesman. Police searched a vehicle that was parked in a no parking zone, finding a digital scale with suspected marijuana residue inside the glove box. The officers also found a black Nike shoe box in the trunk with 33 credit cards inside. Several of the credit cards did not have holograms or security codes and appeared to be forged, police said. Source: http://www.hometownannapolis.com/news/top/2010/07/09-18/Police-uncover-fake-credit-card-operation.html

Newest attack on your credit card: ATM shims. Shimming is the newest con designed to skim a person's credit card number, PIN and other info when one swipes a card through a reader like an ATM machine. The shim is the latest attack being used by criminals to steal info at the ATM or other Pin Entry Device. According to Diebold, "The criminal act of card skimming results in the loss of billions of dollars annually for financial institutions and card holders. Card skimming threatens consumer confidence not only in the ATM channel, but in the financial institutions that own compromised ATMs as well." Shimming works by compromising a perfectly legitimate card reader (like an ATM) by inserting a very thin flexible circuit board through the card slot that will stick to the internal contacts that read card data. The shim is inserted using a "carrier card" that holds the shim, inserts it into the card slot and locks it into place on the internal reader contacts. The carrier card is then removed. Once inserted, the shim is not visible from the outside of the machine. The shim then performs a man-in-the-middle attack between an inserted credit card and the circuit board of the ATM machine. Source: http://www.networkworld.com/community/node/63544

Chemical and Hazardous Materials Sector

DHS initiates first enforcement action of chemical plant safety regulations. The Department of Homeland Security (DHS) initiated its first enforcement actions against U.S. chemical facilities under federal anti-terrorism law. The Department sent letters to 18 chemical facilities warning that their failure to comply with safety regulations may result in heavy fines or worse. The administrative orders sent to the facilities represent the final step before the Department begins prosecution. Under the law, DHS can assess fines of up to $25,000 per day for failure to comply. In addition, the law gives the Department authority to shut down a chemical facility if its owners fail to respond to DHS

requirements for security improvements. A Securityinfowatch reporter wrote that the Department also confirmed that all 18 of the non-compliant sites are in the top tier of facilities considered by federal officials to be most at risk for an attack by terrorists intent on causing massive off-site casualties. A DHS spokesman said the 18 facilities that have failed to produce security plans have been given several reminders, beginning in late 2009, about their obligations. Source: http://homelandsecuritynewswire.com/dhs-initiates-first-enforcement-action-chemical-plant-safety-regulations

HOS exemption proposed for short anhydrous ammonia transport. The Federal Motor Carrier Safety Administration (FMCSA) is taking comments until August 13 on a proposed two-year exemption of some drivers and motor carriers from the federal hours of service regulations when they transport anhydrous ammonia from any distribution point to a local farm retailer or the ultimate consumer, so long as the trip is 100 air-miles or less from the retail or wholesale distribution point. The chemical compound is stored under high pressure and widely used as fertilizer, with users handling it carefully to prevent spills. FMCSA said it has reviewed crash data and believes the exemption "would likely achieve a level of safety that is equivalent to, or greater than, the level that would be achieved absent such exemption, based on the terms and conditions imposed." The exemption would preempt "inconsistent" state and local requirements applicable to interstate commerce, the agency's Federal Register notice stated. To be eligible, a motor carrier would have to have a "satisfactory" safety rating or be "unrated." Drivers for motor carriers with "conditional" or "unsatisfactory" safety ratings could not take advantage of the exemption. Source: http://ohsonline.com/articles/2010/07/16/hos-exemption-proposed.aspx?admgarea=news

Implementation guidance for physical protection of byproduct material; Category 1 and Category 2 quantities of radioactive material. The Nuclear Regulatory Commission (NRC) is proposing to amend its regulations to establish security requirements for the use and transport of category 1 and category 2 quantities of radioactive material. In a July 14 Federal Register notice, the NRC spelled out draft guidance to address implementation of the proposed regulations. The notice announces the availability of the draft implementation guidance document for public comment. Source: http://edocket.access.gpo.gov/2010/2010-17126.htm

Many ways to smuggle nukes into the United States. The United States focuses on scanning shipping containers for nuclear smuggling, and with nearly 10 million cargo containers arriving in the United States by sea or on land each year, this is a difficult task experts acknowledge. But the Government Accountability Office (GAO) said this work is not enough, calling on the government to find ways to keep an eye on 13 million recreational boats and 110,000 fishing vessels which go in and out U.S. seaports — as well as on freight trains that are often more than three kilometers long. Terrorists bent on smuggling nuclear materials into the United States still have plenty of ways to do so, beyond shipping containers, the GAO stated in a new report. "It is important to close these gaps because dangerous quantities of nuclear materials can be portable enough to be carried across borders by vehicles or pedestrians on most private aircraft or small boats," the director of the GAO's natural resources and environment division, testified in a Congressional hearing that discussed the study. Source: http://homelandsecuritynewswire.com/many-ways-smuggle-nukes-united-states

(Texas) **OSHA cites Enbridge G&P following worker fatality from hydrogen sulfide.** The Occupational Safety and Health Administration (OSHA) has cited Enbridge G&P LP with two alleged

willful and five alleged serious violations following a chemical release at the company's Bryans Mill plant in Douglasville, Texas, which resulted in a worker's death. OSHA began its investigation January 10 following the fatality that occurred when four workers were replacing a faulty valve on the waste heat boiler in the sulfur plant. One employee died and another was left in critical condition when hydrogen sulfide was released from the boiler. The willful violations were issued for failing to develop and implement safe work practices for workers who process equipment or piping or who are exposed to airborne concentrations of hydrogen sulfide in excess of 50 parts per million, and for failing to provide workers with the required personal protective equipment. In this case, the company did not provide respirators. Alleged serious violations include failing to review current operating procedures; to inform contract workers of the known potential fire, explosion or toxic release hazards related to the contractor's work; and to use flame-resistant clothing when breaking lines, valves and/or opening equipment. For these violations, OSHA has assessed penalties totaling $152,100. Enbridge G&P has 15 business days from receipt of citations to comply, request an informal conference with the OSHA area director in Dallas or contest the citations and penalties before the independent Occupational Safety and Health Review Commission. Source: http://ehstoday.com/standards/osha/osha-enbridge-gp-worker-fatality-hydrogen-sulfide-8237/

Napolitano makes push for CFATS. Speaking the week of July 5 at the Chemical Sector Security Summit in Baltimore, the Department of Homeland Security (DHS) Secretary lauded progress made by partnerships forged between government and the private sector in ensuring chemical plant security, citing in particular the efficacy of "flexible, practical and collaborative programs such as DHS' National Infrastructure Protection Plan, the Chemical Sector Coordinating Council and, especially, the Chemical Facility Anti-Terrorism Standards (CFATS)." Going forward, the Secretary added that cybersecurity, in addition to physical security measures, would emerge as a key part of any critical infrastructure security strategy. The Secretary's remarks came only a week after DHS began a major offensive on enforcement of CFATS against chemical companies failing to conform with the security regulations, established by DHS in 2007. In late June, DHS sent 18 chemical companies orders to complete site-security plans for their facilities within 10 days. CFATS regulations mandate that private companies must make a full inventory assessing their potential vulnerabilities. Companies found to be at highest risk then are required to develop site-security plans and take other protective measures, after which they are periodically audited by DHS. Since the creation of CFATS, DHS has received site-security plans from more than 1,000 companies. Source: http://www.hstoday.us/content/view/13916/149/

Commercial Facilities

(Pennsylvania) **Bethlehem bomb squad disables suspicious box with clock strapped to it at Via of the Lehigh Valley.** On July 14 the Bethlehem, Pennsylvania bomb squad disabled a suspicious box with a clock strapped to it that arrived at Via of the Lehigh Valley among donated items. The package arrived at the organization's headquarters on a delivery truck that had picked up donations at Via donation boxes throughout the Lehigh Valley. Via'S interim director said that an employee carried the package, about the size of a shoe box, outside and called 911. The package was not ticking. The agency evacuated its offices and coordinated a change in pick-up and drop-off locations for its clients. About 120 people were in the offices at the time of the evacuation. Via, a nonprofit that provides a host of services for children and adults with disabilities, said it is not certain at which one of its 13 drop-off location the package was found. Via collects donations almost daily. Police were dispatched

to the Via building at 2:18 p.m. The bomb squad had disabled the "device" but would not comment as to whether the package was indeed an explosive device until the police and bomb squad completed an investigation. During the investigation, police ordered Route 378 closed between Eighth Avenue and the Hill-to-Hill Bridge due to the package's proximity to the expressway. Police also closed a portion of Union Boulevard. Source: http://www.lehighvalleylive.com/bethlehem/index.ssf?/base/news-2/1279166750251130.xml&coll=3

(Kansas) **Sheriff's audience evacuated after suspicious package found.** A suspicious package prompted authorities to evacuate a Kansas convention center where a controversial Arizona sheriff was speaking, a police spokesman said July 13. Later that evening, the FBI gave the all-clear. "A suspicious package was noticed and in an over-abundance of caution, we took all the precautions necessary because it was suspicious package," the spokeswoman said. The package was not an explosive device. An Overland Park Police spokesman said the bomb squad removed the package and contained it, and police evacuated the parking lot to conduct a thorough sweep to look for any other suspicious items. The spokesman could not say where the package was found. The Maricopa County, Arizona Sheriff was to speak at the Ritz Charles Convention Center in support of a Kansas secretary of state candidate, who says he helped write Arizona's controversial legislation that requires law enforcement to ascertain the immigration status of those under investigation if the officers believe the suspects are in the country illegally. Source: http://www.cnn.com/2010/US/07/13/kansas.arpaio.suspicious.package/

(Iowa) **Bomb squad probes suspicious object in Pleasant Hill.** The Des Moines, Iowa Bomb Squad helped Pleasant Hill police disarm an object resembling a bomb July 10 at Sleepy Hollow Sports Park. Maintenance workers called police after discovering the item at the hangman's gallows on the outskirts of the Sleepy Hollow Renaissance Fair. According to police reports, the object was a plastic toolbox containing two gas cylinders. On top of the cylinders were a kitchen timer and a circuit board. A responding Pleasant Hill police officer determined the item appeared to be a time bomb, cleared the area, and requested a bomb squad. The bomb squad used a robot to inspect the device, take an X-ray, and then disrupt the device. Pleasant Hill police searched the area, and the item was placed in storage for further investigation. Source: http://www.desmoinesregister.com/article/20100712/NEWS/7120324/-1/LIFE04/Bomb-squad-probes-suspicious-object-in-Pleasant-Hill

Are Somali militants behind the Uganda blasts? Simultaneous explosions tore through crowds watching the World Cup final in the Ugandan capital of Kampala July 11, killing 64. Somali Islamic militants are expected to have carried out the the bombings, one at a rugby club, where 49 people died, and the other at an Ethiopian restaurant, where 15 were killed. A spokesman for the Ugandan government said vests and body parts at the scenes indicated the work of suicide bombers. The U.S. embassy in Kampala confirmed that one American was among the dead at the restaurant. A church group from Pennsylvania was inside at the time, according to the Associated Press, and several Americans were among the scores of wounded. The Kampala police chief suspected that Somali extremist group al-Shabab was behind the bombings. While al-Shabab is a fragmented organization and no one leader speaks for all its factions, a spokesman for al-Shabab in Kismayo, southern Somalia told TIME, "This is the work of mujahedin. We were happy with those guys who did that. God will reward them." He did not confirm that al-Shabab was responsible for the attacks, but he did say the

bombings were in response to calls in the region for a stronger international force to intervene in Somalia's ongoing civil war. At the start of the World Cup, al-Shabab threatened to execute anyone caught watching a broadcast of the tournament in Mogadishu because it deemed the tournament frivolous Western entertainment. Source: http://www.time.com/time/world/article/0,8599,2003120,00.html#ixzz0tTHs5mxj

(Texas) **Suspicious package found at Fort Worth church.** The Fort Worth, Texas bomb squad was called to an east-side church July 11 after a worker opening the Mount Moriah Baptist Church found a suspicious device. The package was described as several electronic devices — including a camera and a clock — connected with wires and some canisters. Church members arriving for services were turned away as the bomb squad's robot disassembled the device and found it to be harmless. Fire department investigators said it may have simply been a collection of forgotten tools. But the Mount Moriah pastor feels that what happened was certainly no accident. No one saw the package when the church was locked up the previous night. In the end, investigators determined the package was not dangerous. Their focus now is figuring out whether it was all a harmless mistake or a deliberate attempt to intimidate. Source: http://www.wfaa.com/news/local/bum-98207534.html

(Indiana) **Grenade successfully detonated by Toledo Bomb Squad at Nettle Lake.** A live hand grenade from the Vietnam era was safely detonated July 10 after children found it at Nettle Lake in Williams County, Indiana. A Nettle lake resident called police at 5:20 p.m. to report the incident. Deputies and firefighters verified the device was a hand grenade and secured the area for public safety. A bomb squad from the Toledo Police Department arrived and worked with the U.S. military to determine that the grenade was an explosive device from the Vietnam era. Bomb technicians dug a hole and lined it with concrete before moving the grenade into the hole and detonating it at 11 p.m. A piece of concrete struck a nearby lake cottage, causing minor damage, police said. The Williams County Sheriff's Department was assisted by the Northwest Township Fire Department and Williams County EMS. Source: http://www.journalgazette.net/apps/pbcs.dll/article?AID=/20100711/LOCAL07/100719968

Communications Sector

Nothing Significant to Report

Critical Manufacturing

Ford Motor, Chrysler recall vehicles. Ford Motor Co. is recalling 33,700 of its Transit Connect small commercial vans over an interior liner, while Chrysler Group said it was recalling certain 2010 SUVs and trucks over a possible brake fluid leak. Ford is recalling the Transit Connect vehicles sold in the United States and manufactured from December 2008 through May 2010 due to an interior liner that fails to meet all safety requirements for head protection. Separately, Chrysler is recalling certain 2010 Jeep Liberty and Wrangler, Dodge Nitro and Ram 1500 trucks made in the U.S. that may have been built with an improperly formed tube that could cause brake fluid to leak. Chrysler is halting sales of the affected vehicles, made in April and May, until the problem covering up to 22,000 vehicles is fixed, the company said in a letter to regulators. Source: http://www.reuters.com/article/idUSTRE66847J20100709?type=domesticNews

(New Mexico) **Police: 6 dead, 4 wounded in Albuquerque shooting.** A gunman opened fire at an Albuquerque fiber optics manufacturer July 12, killing six people and wounding four others before killing himself in what police said was a domestic violence dispute. The shooting at Emcore Corp. appeared to involve the gunman's ex-wife or girlfriend, who was among the dead, the police chief said. The gunman was a former employee. Chaos unfolded as the gunman opened fire, sending employees fleeing for cover as police locked down the entire neighborhood. Police said 85 employees were later taken to a community center for interviews with detectives. Six victims were taken to University of New Mexico Hospital. Emcore manufactures components that allow voice, video and data transmission over fiber optic lines. They also manufacture solar power systems for satellite and ground-based systems. Based in Albuquerque, the company has about 700 full-time employees. Source: http://www.google.com/hostednews/ap/article/ALeqM5gGyymIn9tYQq6i5YEfDoNvuRRnfQD9GTLNQ00

Defense/ Industry Base Sector

JSF heat woes being fixed. Changes are being made to the integrated power package (IPP) on the Marine's F-35 that should limit heat damage to carrier decks and other surfaces by reshaping the nozzle so that the enormous thrust comes out in an oval shape instead of the more highly focused circle now used. The oval "will resolve that problem for almost all surfaces," the Marines' deputy commandant for aviation told DoD Buzz. An operational assessment of the JSF said that heat may force "severe F-35 operating restrictions and or costly facility upgrades, repairs or both." The OT-IID report said "thermal management" will "increase the number of sorties required to prepare an operational unit for deployment during summer months" at most American bases. Source: http://www.dodbuzz.com/2010/07/19/jsf-heat-woes-being-fixed-trautman/

(Florida) **Thousands of laptops stolen during nine-hour heist.** Thousands of laptops have been stolen from the Tampa, Florida office of a private contractor for the U.S. military's Special Operations Command. Surveillance cameras caught up to seven people loading the computers into two trucks for nine hours. U.S. Special Operations Command coordinates the activities of elite units from the Army, Navy, Air Force and Marines. A spokeswoman said July 13 that none of the stolen laptops contained military information or software. The Virginia-based company iGov was awarded a $450-million contract earlier this year to supply mobile-technology services linking special operations troops worldwide. A company executive said iGov is cooperating with authorities and the March 6 break-in at its Tampa facility remains under investigation. Source: http://www.google.com/hostednews/ap/article/ALeqM5jBQCXgAk_-2NyNZdtPSi8a1HmwaQD9GUB8RO0

(Florida) **Research park adapts to anti-terrorism makeover.** For nearly two years now, Central Florida Research Park in east Orange County has been quietly and subtly transforming some of its most prominent facilities into anti-terrorism fortresses for the high-tech military agencies located there. Security measures such as vehicle-resistant fences, steel entrance gates and concrete pylons have been installed with the aim of hardening what the military calls "soft" targets for terrorism. The research park, next door to the University of Central Florida in Orlando, was a prime candidate for enhanced security, with its military complex built into in a suburban setting that is part college campus, part office park. The project is the result of a Pentagon edict, issued after the September 11,

2001, terrorist attacks, calling for security upgrades at any building with a substantial military presence. Much of the work was paid for by the Pentagon itself, including improvements at the military's 280,000-square-foot, high-tech, training-systems complex, which contains major Navy and Army contracting units, as well as other military agencies. Source: http://www.orlandosentinel.com/business/breakingnews/os-cfb-cover-research-park-071210-20100711,0,1923194.story

Boeing F-15 Silent Eagle demonstrator makes 1st flight. The Boeing Company Silent Eagle flight demonstrator aircraft F-15E1 completed a successful first flight July 8 from Lambert St. Louis International Airport. During the 80-minute flight, F-15E1 opened and closed its left-side Conformal Weapons Bay, which contained an AIM-120 Instrumented Test Vehicle (ITV) missile. The ITV was not launched. "The Silent Eagle demonstration flight validated our initial engineering design approach," said Boeing's F-15 development programs director. Source: http://nosint.blogspot.com/2010/07/boeing-f-15-silent-eagle-demonstrator.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence)

Emergency Services

(California) **Sniper targets Oakland cops.** Oakland, California police have their hands full. In addition to a shootout on the freeway and a police-involved shooting at a BART station, officers are now on the hunt for an apparent sniper trying to take out officers. The latest incident happened July 18 at about 11:30 p.m. Patrol officers were on a traffic stop near 8th and Adeline Streets in West Oakland when they heard shots. They were detaining people in a car on suspicion of drug-related offenses. The officers had to get out of the line of fire and get the detainees out of the line of fire. They called for back up. Police searched the high-rise apartment building from where they believe the shots were fired but they did not find the gun or the shooter. To make matters worse, police checked the building's security room where cameras might be — and the room had been vandalized. Police said it is unclear whether that was done in advance by the shooter or if it was a coincidence, but they were not able to get any surveillance tape right way which might help in the investigation. The officers and detainees were not hit. Source: http://www.msnbc.msn.com/id/38308005/ns/local_news-san_francisco_bay_area_ca/

Safety concerns, shortage of pilots slow use of aerial drones along borders. Safety concerns and a shortage of drone pilots has slowed the integration of unmanned aerial vehicles (UAVs) into security plans for the U.S.-Mexican border, officials told a House Homeland Security panel July 15. Federal Aviation Administration (FAA) officials said the UAVs operated in U.S. airspace were initially designed for military applications. While the technology has advanced, "their safety record warrants careful review." There are six Predator B UAVs operated by civilian agencies along the northern and southern borders. A seventh is expected to be delivered this year, and another is included in the U.S. President's budget blueprint for Fiscal Year 2011, which begins October 1. FAA officials said Border Patrol has had seven reported deviations this year, where the aircraft made an unplanned or unexpected move that violated airspace regulations. Source: http://www.dallasnews.com/sharedcontent/dws/news/texassouthwest/stories/DN-drones_16tex.ART.State.Edition1.2951c5c.html

Secretary Napolitano announces more than $1.8 Billion in fiscal year 2010 preparedness grants. The Department of Homeland Security (DHS) announced July 15 more than $1.8 billion in Fiscal Year (FY) 2010 Federal Emergency Management Agency preparedness grants designed to help states, urban areas, tribal governments and non-profit organizations enhance their protection, prevention, response and recovery capabilities for risks associated with potential terrorist attacks and other hazards. The Homeland Security Grant Program is the Department's primary funding mechanism for building and sustaining national preparedness capabilities to help strengthen the nation against the risks associated with potential terrorist attacks and other hazards. Additionally, 80 percent of Operation Stonegarden funding –- intended to support state and local law enforcement along the border –- will go to Southwest border states. DHS also increased tribal funding from $1.8 million in FY 2009 to $10 million in FY 2010. Source:
http://www.dhs.gov/ynews/releases/pr_1279205905487.shtm

(Florida) **Unfounded bomb threats give authorities busy day.** People were evacuated from two government facilities in Tavares, Florida July 14, including the Lake County Sheriff's Office, after bomb threats were called in. Nothing was found and everyone is safe, police said. The first threat was called into the state Department of Children and Families (DCF) facility at 1300 S. Duncan Drive. DCF employees then called Tavares police about 8 a.m. Authorities also investigated a bomb threat at the Lake County Sheriff's Office. A deputy and a K-9 searched the common areas of the main sheriff's office building at 360 W. Ruby St. and the jail on Main Street, but found nothing, a sheriff's lieutenant said. No one was evacuated. Source:
http://www.dailycommercial.com/localnews/story/071510bombthreats

(Massachusetts) **Man arrested after bombs found in Hopkinton.** A man suspected of causing bomb scares July 9 at the Hopkington, Massachusetts police station and in a quiet neighborhood, was arrested as experts disabled two improvised explosive devices. A bomb squad worked on Downey and Main streets while police obtained a warrant and arrested a town resident. Police had taken the suspect into protective custody earlier in the morning at a West Main Street business and found a "suspicious device" on him, according to a department press release. Officers took the device outside, secured the area and eventually released the suspect. Then, around 8:40 a.m., authorities responded to Downey Street, where a resident reported finding what may have been a bomb wedged into his camper. The device, a little bigger than a beer can, contained BBs, nails and rocks. It had been lit but didn't blow up. Had it done so, it could have caused serious injuries, a fire chief said. Source:
http://www.metrowestdailynews.com/news/x104355480/Suspected-explosive-devices-found-in-Hopkinton

ENERGY

(Massachusetts) **Bomb scare shuts down Broadway gas station in Raynham.** The Massachusetts state bomb squad and local emergency crews rushed to a Raynham gas station early July17 after receiving a call that a suspicious package making a "siren-like noise" was found next to one of the pumps. Raynham police and firefighters arrived at Gulf Gas at 5:30 a.m. to find a 10-square-inch cardboard package that appeared to have electronic parts attached to it. An ambulance was also dispatched to the scene as a precaution. Officers secured the area and called in the state police bomb squad. A remote-controlled robot moved the package to a secure location for detonation. There were

electronics and batteries but no explosives in the package, police said. The state fire marshal's office is continuing the investigation. Source: http://www.wickedlocal.com/mansfield/topstories/x1005406082/Bomb-scare-shuts-down-Broadway-gas-station-in-Raynham

(Texas) **Energy sector tie revealed for pipe bomb attack.** Federal agents have expanded their investigation into a weekend pipe bomb attack after finding out the victim may have been targeted because her husband is president of a local oil company, Local 2 Investigates reported July 12. The victim was rushed to the hospital after the July 9 explosion on the family's porch in northwest Houston. She is the wife of the president of Adams Resources Exploration, according to investigators. The company focuses on exploration and development in the Gulf of Mexico, off the coast of Texas and Louisiana. Adams is based in Houston. Local agents with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) said they could not comment on this new development. ATF agents are coordinating with Houston Police Homicide Squad investigators and the Houston FBI since the scope of the investigation shifted completely with the possible energy sector tie. The Houston FBI said it is coordinating with ATF, but that ATF is the lead agency on the investigation since an explosive was involved. An FBI spokeswoman said the ATF is in charge because terrorism was ruled out. Federal and local investigators said they have not conclusively determined that the family's energy ties were the reason for the attack, and investigators have not revealed any extortion attempt or other dispute prior to the bombing. Source: http://www.click2houston.com/investigates/24228830/detail.html

Senator warns of terrorist threat to oil rigs. A Democrat Senator from Virginia is calling on the U.S. President to develop plans to safeguard offshore platforms from attack by terrorists. While the BP oil disaster in the Gulf of Mexico has put accidental spills squarely in the national spotlight, the Senator is warning of another possible threat: deliberate sabotage. The Senator, a member of the Senate Armed Services Committee, made his case in a letter to Defense Secretary Robert Gates, Homeland Security Secretary Janet Napolitano and Interior Secretary Ken Salazar. "While Congress will continue to scrutinize BP and regulatory agencies, I write to urge you to also be vigilant against deliberate acts, such as an attack or sabotage, that could similarly devastate the region," the Senator said in the letter, referring to the Gulf Coast. But he wants the security plans adopted for all U.S. coastal areas. He's asking federal agencies to assess how vulnerable offshore oil rigs are to attack, and to make recommendations for safeguarding them. Source: http://www.cnn.com/2010/US/07/13/offshore.rigs.security/

(Georgia) **Training kept pipeline blast from being bigger disaster.** The McDuffie County, Georgia fire chief had never worked a pipeline fire before last week, but he was prepared when he got the call. Each August, firefighters gather to learn about the dangers and strategies for working pipeline disasters. "Because of that we were able to minimize the situation a little bit," said a Dixie Pipeline spokesman. "That was a tremendous help." Firefighters already knew where emergency valves were located when they arrived at a Thomson propane pipeline explosion July 5. After quickly getting permission from Dixie representatives, the fire chief was able to shut down the valves. Firefighters cased the perimeter and determined an evacuation of the area wasn't necessary. Source: http://chronicle.augusta.com/news/metro/2010-07-10/training-aided-dousing-pipeline?v=1278846722

(Kentucky) **Thieves use backhoe to steal copper from substation.** Crooks used a backhoe to steal copper from a Bluegrass Energy substation on Harrodsburg Road in Jessamine County, Kentucky July 12. A security guard at a nearby farm called 911 when he heard a beeping sound, believed to be coming from the backhoe. The thieves had somehow gotten inside the substation then started the backhoe to lift the spool over the fence. For some reason, the crooks didn't take the entire spool. It is believed they got away with some copper, but it is not yet known how much. When the security guard went to check out the noise, the thieves were already driving away in a car without headlights. He didn't get a good description of the car. Source: http://www.wkyt.com/home/headlines/98229349.html

Food and Agriculture

(California; National) **Bagged salad recalled for possible E. coli contamination.** Certain bagged salads and lettuces are being recalled due to a possible E. Coli contamination. Fresh Express is recalling 23 varieties of Romaine salads with expired "use by" dates of July 8-12, and have an "S" in the product code, according to the Salinas, California company. No illnesses have been reported. The recall was announced in response to a positive E. Coli reading in a random bagged lettuce sample test conducted on behalf of the U.S. Food and Drug Administration. The lettuce was distributed to retailers in 19 states, including California. Retailers have been instructed to remove the possibly affected salads from store shelves. Source: http://www.ktla.com/news/landing/ktla-salad-recall,0,4379553.story

Kellogg cites packaging chemical in cereal recall. Kellogg Co. said July 14 that higher-than-normal amounts of certain chemicals in its package liners caused the unusual smell and flavor that prompted a recall of 28 million boxes of its cereal in late June. The food maker recalled Apple Jacks, Corn Pops, Froot Loops and Honey Smacks after about 20 people complained, including five who reported nausea and vomiting. Consumers reported the cereal smelled or tasted waxy, and others said the taste or smell was similar to that of metal or soap. Other people simply described the taste as stale. The company, based in Battle Creek, Michigan, said it has identified elevated levels of chemicals called hydrocarbons as the source. Those chemicals include methyl naphthalene. Little is known about the risks of moderate exposure to methyl naphthalene. The Food and Drug Administration said it is reviewing Kellogg's information and conducting its own risk assessment. Source: http://www.forbes.com/feeds/ap/2010/07/14/general-specialized-consumer-services-us-kellogg-cereal-recall_7768048.html?boxes=Homepagebusinessnews

(Wisconsin) **Salmonella outbreak in Kenosha.** The Kenosha County Health Department in Wisconsin is investigating an outbreak of salmonella, which has been confirmed in 26 residents, the department said July 14. Salmonella, a type of bacteria, is transmitted to humans when they eat foods contaminated with the bacteria. The illness usually lasts four to seven days and often goes away without treatment. Each year, approximately 40,000 cases of salmonella are reported in the U.S. Source: http://www.journaltimes.com/news/local/article_8ea3842c-9006-11df-8a15-001cc4c03286.html

Public health advocates press Senate to pass food safety bill. A year after House Democrats and Republicans overwhelmingly approved legislation to improve food safety, public health advocates are

growing frustrated that the Senate has yet to take up the bill. A coalition of food-safety groups tried to turn up the pressure last week on the Senate majority leader and minority leader, running newspaper ads in the lawmakers' states — Kentucky and Nevada — featuring constituents who fell seriously ill from food poisoning. The ads urged the senators to move the bill to the Senate floor and pass it.On July 14, the U.S. President said in a prepared statement that he supported passage of the Senate bill, and that it would give the government the tools it needs to ensure food safety. The bill, which would be the first major change to food safety laws in 70 years, is designed to give the Food and Drug Administration vast new regulatory authority over food production. It places greater responsibility on manufacturers and farmers to produce food free from contamination — a departure from the country's reactive tradition, which has relied on government inspectors to catch tainted food after the fact. The legislation follows a wave of food-borne illnesses over the past four years, involving products as varied as spinach and cookie dough, which has shaken consumer confidence and made the issue a priority for many lawmakers and the White House. Food illnesses affect 1 in 4 Americans and kill 5,000 each year, according to government statistics. Source: http://www.boston.com/news/health/articles/2010/07/12/public_health_advocates_press_senate_to_pass_food_safety_bill/?rss_id=Boston.com+--+Health+news

Australian vegetables poisoned as police probe sabotage. Police in Australia are investigating the poisoning of 7 million vegetable seedlings, including tomatoes, aubergines and melons. Detectives believe a herbicide was injected into the irrigation system at a nursery in northern Queensland. The poisoning was the fourth such incident in eight years. Farmers and analysts say the price of vegetables will increase as a result. The cost of the damage is estimated at $20.3 million. Police are investigating possible links to the other poisonings in the region, which produces most of Australia's vegetables during the winter months. The bulk of the poisoned plants - around 4 million - were tomato seedlings. Some of them had already been transplanted on farms. Around 350 hectares of production land, with the capacity to grow about 200 tons of fresh produce, have been affected. The vegetables were destined for sale across Australia and for export to New Zealand and the Pacific island nation of Vanuatu. Prices in all three countries are likely to spike over the next few months until produce from other regions comes onto the market, reports say. Source: http://news.bbc.co.uk/2/hi/world/asia_pacific/10559447.stm

Miravalle Foods Inc. recalls peppers because of possible health risk. Miravalle Foods, Inc. of S. El Monte, California has recalled 37,318 lbs. of "Miravalle Chile California & Miravalle Chile Nuevo Mexico Brand Peppers" distributed between March 15 and May 6 to some customers in California, Colorado, Utah, North Carolina, Nebraska, Idaho, Oregon and Nevada because they may be contaminated with Salmonella. The recalled peppers were distributed to a small group of customers through direct delivery, distributors and retail stores. They are in bulk 25 lb. boxes, and varying sizes of clear plastic packages under the Miravalle Chile California & Miravalle Chile Nuevo Mexico" brand, including: 3oz. (UPC Code: 7 12810-00301 & 7 12810-00304), 6 oz. (UPC Code: 7 12810-60001 & 7 1280-60004), 8oz. (UPC Code: 7 12810-00802 & 7 12810-00803) and 16 oz. (UPC Code: 7 12810-16005 & 7 12810-16007) packages. No illnesses have been reported. The recall was issued after lab analysis of a random sample conducted by the U.S. Food and Drug Administration (FDA) revealed the presence of Salmonella. Production of the product has been suspended while the FDA and the company continue to investigate, Consumers who have purchased the peppers are urged to return them to the place of purchase for a full refund. Consumers with questions may contact the company

at 1-626-575-7551 between 8 a.m. and 4 p.m. PST. Source: http://www.fda.gov/Safety/Recalls/ucm218474.htm

(Florida) **Horse disease prompts alert.** Three fatal cases of eastern equine encephalitis (EEE) on the Ridge has prompted a health advisory to be issued for both horses and residents in Polk County, Florida. The disease claimed a horse in rural Lake Wales and another in rural Frostproof. Neither horse had been vaccinated for the disease, according to local and state medical officials. A spokesperson for the state health department confirmed that an additional fatal equine case in Polk occurred in April. In that case, the horse previously had been inoculated but was not current on its shots. To date, 32 cases of EEE have been confirmed statewide. One veterinarian noted that once a horse is infected and a veterinarian is called, it is usually much too late to save the animals. Although rare, the disease can also be spread to humans, according to the health department. So far, no human cases have been reported. Source: http://www.lakewalesnews.com/articles/2010/07/10/county_page/doc4c3779a97c144228374951.tx

(California; Hawaii) **J. Hellman Frozen Foods, Inc. recalls avocado pulp due to possible health risk.** J. Hellman Frozen Foods, Inc. of Los Angeles has recalled 992 cases (4,960 retail units) of SeÃ±or Mexicanoâ.¢ Avocado Pulp, because it may be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections. The avocado pulp was distributed in California and Hawaii, and includes 2 lb. bags of SeÃ±or Mexicanoâ.¢ Avocado Pulp, (UPC Code 7 503012 650001), with the Lot number A 21 04 10 / A 21 04 12. There have been no illnesses reported. The recall was issued based on a confirmed positive result for Listeria in a random sample test conducted by the U.S. Food and Drug Administration. J. Hellman has notified its customers and directed them to remove the product from their shelves. Consumers should dispose of the product or return it to the place of purchase for a refund. People with comments or concerns should contact J. Hellman's director of food safety at 213â..243â..9105 between the hours of 4 a.m. and 9:30 a.m. Source: http://www.fda.gov/Safety/Recalls/ucm218455.htm

(Kentucky) **Clover-linked condition killing cattle across Bluegrass.** It's been a tough year so far for Central Kentucky's cattle producers as they struggle to contain a potentially fatal condition called "frothy bloat" that has taken a toll on herds. The damage has become so severe that state officials have petitioned the U.S. Department of Agriculture to include the condition in a program that allows farmers to request federal reimbursement for losses. In general, the cattle affected by frothy bloat, technically called primary ruminal tympany, have eaten too much clover. Though clover improves pasture quality, ingesting too much of it can be damaging because it can cause fermentation gases to be trapped inside the cattle's rumen, or stomach. The clover produces a foam inside the cattle's gastrointestinal tract that prevents them from being able to burp. When the gas can't escape, the rumen expands, much like a balloon, and presses on the diaphragm. That can lead to suffocation. A survey suggests that just 1 percent of the cattle represented had died, but an extension beef cattle specialist at the University of Kentucky extrapolated from the results and national data to estimate that means losses of almost $5 million. Source: http://www.kentucky.com/2010/07/11/1344802/clover-linked-condition-killing.html

Government Sector (including Schools and Universities)

(Iowa) **Personal details of 93,000 staff and students at university could be exposed after database compromise.** The personal details of 93,000 people have been exposed, following the compromise of a database a college in Storm Lake, Iowa. The social security numbers, addresses and driver's licence information of students and staff at Buena Vista University dating back to 1987 could be vulnerable, according to whotv.com. It further claimed that the unauthorized access was confirmed last month and the university began notifying those potentially affected. Despite the breach, university officials said that there has not been any indication that the information has been misused. The incident is being investigated by a computer forensics team, while attorneys are also reviewing the matter. The Buena Vista president has apologized for the incident, and said that the university is trying to mitigate potential harm. Source: http://www.scmagazineuk.com/personal-details-of-93000-staff-and-students-at-us-university-could-be-exposed-after-database-compromise/article/174841/

(North Carolina) **Coast Guard looks to ID prank caller.** The Coast Guard is seeking the public's help to identify individuals responsible for recent false distress calls in North Carolina. Sector North Carolina watchstanders overheard two men talking on their marine VHF radios about making false distress calls to the Coast Guard. One of the men admitted to previously making a false distress call to the Coast Guard. During the conversation, one man said he was told by the Coast Guard to get off the radio after he said, "Mayday, mayday, ship going down." False distress calls limit the Coast Guard's ability to respond to actual emergencies. They also unnecessarily endanger the lives of responders and waste thousands of taxpayer dollars annually, Coast Guard officials said. Source: http://www.newbernsj.com/news/coast-88961-guard-distress.html

(Nevada) **Courthouse reopens after bomb threat in Las Vegas.** Local and state courts opened two hours late in Las Vegas after a regional courthouse was locked down for the investigation of a telephoned bomb threat. Police and court marshals said July 14 that no device was found and hundreds of people were allowed inside the 17-story regional justice center after a safety sweep. The court marshal said a bomb call came in about 7:15 a.m. A Las Vegas police spokesman said a man telephoned 911 and said an explosive device had been smuggled into the downtown courthouse during the last 10 days. The spokesman said the man hung up without giving his name. Source: http://www.lasvegassun.com/news/2010/jul/14/courthouse-reopens-after-bomb-threat-in-las-vegas/

Missouri to host National Guard Homeland Response Force. The Department of Defense (DOD) has selected Missouri to host a National Guard Homeland Response Force. Ten Homeland Response Forces will be located across the nation in each of the 10 Federal Emergency Management Agency (FEMA) regions. The creation of the Homeland Response Force is a part of DOD's larger reorganization of its domestic chemical, biological, radiological, nuclear and high yield explosive (CBRNE) consequence management enterprise, initiated during the 2010 Quadrennial Defense Review. This reorganization will ensure DOD has the ability to respond rapidly to domestic Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons incidents while recognizing the primary role that the governors play in controlling the response to incidents that occur in their states. The Missouri Homeland Response Force will be established in Fiscal Year 2012. Each Homeland

Response Force will be comprised of approximately 570 personnel and will respond within 6 to 12 hours of an event. Its mission will be to provide life-saving medical, search and extraction, decontamination, security, and command and control capabilities. Source: http://www.globe-democrat.com/news/2010/jul/13/missouri-host-national-guard-homeland-response-for/

University databases in the bull's eye. A high-profile breach announced during the week of July 5-9 at the University of Hawaii (UH) Manoa was the latest in a rash of summertime university database exposures — and it serves as a reminder of how much work postsecondary institutions still must do to improve their data-security practices, according to experts. The UH Manoa breach affected approximately 53,000 students, faculty, and other customers of the university's parking facilities. It was the result of a hacker gaining entry into a server containing a database full of parking-facility customer data, including Social Security numbers and credit-card data. This spate of breaches at higher-education institutions is hardly a surprise to security experts. "When you think about it, educational institutions have a wealth of information," said the vice president of global marketing for Application Security Inc. "They obviously have records on the students themselves, they have Social Security numbers, they have health records, and they also have financial information from the parents who are paying the bills. So they have a lot of very marketable data, which makes them a very attractive target." The Social Security numbers, in particular, are a hot-button issue. Many universities have historically repurposed the numbers as student identifiers — a practice that has been abandoned by most organizations in light of the dangers it puts on student records. Source: http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=225702686&subSection=Attacks/breaches

Information Technology and Telecommunications

Watch out for phone scam that offers tech support, leaves spam. A tricky phone solicitor posing as Microsoft tech support can turn one's computer into a spam-sending zombie machine, and the victim might be charged for it. The scam is one of many fishy attempts to obtain personal information or hack computers, according to a spokeswoman for the consumer affairs unit at a San Jose, California-area district attorney's office. A Santa Cruz man said he recently got the scammer's call. The caller, possibly East Indian, said he was from Microsoft and that the man's computer operating system had errors in it that he could help correct. The Santa Cruz man said he hung up because he had not called Microsoft for assistance and was not having trouble with his computer. The scam has surfaced across North America, in the United Kingdom and in Australia. The caller pretends to be tech support from a computer company, but the instructions he walks people through actually install new software that gives him remote access to the computer, so he can use it to send spam or access people's personal information. Source: http://www.mercurynews.com/breaking-news/ci_15497948?nclick_check=1

Criminals pushing Rogue anti-Virus disguised as scanned documents. E-Mail messages claiming to be scanned documents are the latest attempt by criminals to push rogue anti-virus malware to the masses. The messages, which claim to come from a Xerox WorkCentre Pro, come with a Zip file that will immediately infect the system if accessed. The Tech Herald noticed the malicious e-mail this morning, while checking a drop account for messages. The attachment is a typical Zip file and the message itself attempts to pass itself off as a scanned document from a Xerox Multi-Function Printer. Firms with a Xerox WorkCentre Pro should be able to determine the message is fake, experts said. The WorkCentre Pro can scan documents to e-mail or FTP accounts if configured to do so, but the

most common scanning format is PDF, followed by TIFF and XPS. A WorkCentre Pro will never send a Zip file as an attachment. It appears that while the malicious messages are going to as many people as possible, the criminals behind the campaign are looking to single out users who use Xerox products in-house as a method of scanning and printing. If downloaded and extracted, the file inside the Zip attachment is clearly an executable. On the Tech Herald's test system, once the file was accessed, Microsoft's Security Essentials flagged it immediately. The malware itself has a low detection rate. Source: http://www.thetechherald.com/article.php/201028/5899/Criminals-pushing-Rogue-anti-Virus-disguised-as-scanned-documents

Employees become the weak link in a cyber crime attack. Employees are now targets within organizations rather than the network. The head of new technologies, identity protection and verification at RSA claimed that employees can not only harm a company by accidental downloads or by leaking data, but they also are the new target of cyber criminals. He said: "The adversary has changed, today it is a very well developed economy in a complex environment that is developed over a number of years. He pointed to the Aurora attack from January, which he said was achieved with a simple phishing attack by targeting the employee and getting a way in. With recent surveys from Sourcefire and Unisys pointing to the threat posed by employees using personal devices, which are generally unmanaged for work purposes, the head of new technologies noted this complicate thing. But when asked if a CISO would tell them to stop using it, he replied: "There is a level of dilemma for the security manager who wants to enable productivity and efficiency but wants to be productive." Source: http://www.scmagazineuk.com/a-new-defence-strategy-needs-to-be-developed-by-businesses-as-employees-become-the-weak-link-in-a-cyber-crime-attack/article/174561/

Cybercriminals increase effectiveness with multi-stage attacks. Cybercriminals have been increasing the effectiveness of their individual outreach by creating multi-stage or blended attacks, which combine messaging and Web elements. They use e-mail or search-engine results to lure victims to sites hosting spam advertising, malware, or phishing. A new Commtouch report analyzes the many methods fraudsters, malware distributors and spammers use to inspire their victims to action, such as leveraging trusted brands like Apple and Google; holidays, or current events, for example, the World Cup international soccer tournament. During Q2, Gmail and Yahoo kept the top spots as far as spoofed domains for e-mail distribution, but they have been joined in the top six by Twitter. The Twitter domain was faked in a widespread mailing designed to lure users to a "password reset" Web page that contained malware. Other highlights from the Commtouch report include: Spam levels averaged 82 percent of all e-mail traffic throughout the quarter, bottoming out at 71 percent at the start of May and peaking at nearly 92 percent near the end of June. These numbers are slightly lower than those detected in Q1 and equate to an average of 179 billion spam messages per day; Pharmacy spam retained the top spot with 64 percent of all spam; and India has surpassed Brazil for the title of the country with the most zombies (13 percent of the world's total). Source: http://www.net-security.org/secworld.php?id=9575

Report: Alleged Russian spy worked for Microsoft. A twelfth alleged Russian spy recently identified by the U.S. government has a tech connection: he worked for Microsoft. The alleged spy has been deported to Russia because federal investigators believe he was "in the early stages" of alleged espionage, The Washington Post reported July 14. The paper's anonymous government source asserted that the allege spy had "obtained absolutely no information" while he was in the United States. He had been in the Seattle area and working for Microsoft as a software tester since October.

Microsoft confirmed to the Post that the suspect was, in fact, an employee since last October. Source: http://news.cnet.com/8301-13506_3-20010488-17.html

Report: Adobe Reader, IE top vulnerability list. The most exploited vulnerabilities tend to be Adobe Reader and Internet Explorer, but a rising target for exploits is Java, according to a report set to be released July 14 by M86 Security Labs. Of the 15 most exploited vulnerabilities observed by M86 Labs during the first half of this year, four involved Adobe Reader and five Internet Explorer, the lab wrote in its latest security report for January through June 2010. Also on the Top 15 list were vulnerabilities affecting Microsoft Access Snapshot Viewer, Real Player, Microsoft DirectShow, SSreader, and AOL SuperBuddy. Most of the exploits were first reported more than a year earlier and were addressed by vendors, "highlighting the need to keep software updated with the latest versions and patches," the report said. More Java-based vulnerabilities have been actively exploited, reflecting attackers' attraction to Java's popularity and broad install base. In the most common attack scenario, browsers visiting a legitimate Web site are redirected by a hidden iFrame or JavaScript to a malicious Web page that hosts a malicious Java applet, according to the report. Meanwhile, attackers are finding new ways to dodge malware-detection mechanisms, the M86 report found. "Over the last few months, we have observed a new technique of code obfuscation that combines JavaScript and Adobe's ActionScript scripting language," which is built into Flash. Source: http://news.cnet.com/8301-27080_3-20010473-245.html

Official calls securing critical infrastructure against cyberattack impractical. Securing the nation's power grid and other computer systems that operate the nation's critical infrastructure against cyberattack is unrealistic, because companies cannot afford to check if suppliers have provided trustworthy products, an intelligence official from the Energy Department (DOE) said July 8. "If you give me influence or control of your hardware or software supply chain, I control your systems," said the DOE's director of intelligence and counterintelligence. "We're going to have to develop strategies [for managing the supply chain] that are consistent with [the assets] that we're trying to protect." Systems that pose a national threat if compromised, including military command-and-control systems and networks-managing weapons, must be built using equipment from trusted companies, he added. He noted that the hardware and software must be checked for security vulnerabilities and possible malicious code that could cause problems. To vet the products would cost more than what private sector organizations likely can afford. The director of intelligence suggested government and companies diversify the pool of suppliers that provide the computer hardware and software that help operate the critical infrastructure. Source: http://www.nextgov.com/nextgov/ng_20100708_3510.php

Spammers made June 'Month of Malware'. The loss of several zombie networks due to legal actions caused spammers to up their criminal activities to make up for lost revenue, making June the month of malware, according to Symantec's State of Spam & Phishing Report of June. In 2010, malware levels never rose above 3 percent of all spam, even on days when malware spam increased. In June, however, malware spam made up almost 12 percent of all spam on the 13th, and topped 5 percent on the 3rd and 15th. Phishing Web sites created by automated toolkits increased about 123 percent from May. The number of non-English phishing sites also grew by 15 percent. Among non-English phishing sites, French and Italian continued to be higher in June. Phishing in French increased by one-fourth, mainly in the E-commerce sector. Source: http://www.thenewnewinternet.com/2010/07/12/spammers-made-june-month-of-malware/

Apple ranks first in surging security bug count. The number of vulnerabilities in the first half of 2010 was close to the number recorded in the whole of 2009, security-notification firm Secunia reports. Apple ranks first, ahead of runner-up Oracle, and Microsoft in the number of security bugs found in all products. During the first six months of 2010, Secunia logged 380 vulnerabilities within the top-50 most prevalent packages on typical end-user PCs, or 89 percent of the figure for the entire year of 2009. Secunia believes the security threat landscape is shifting from operating system vulnerabilities to bugs in third-party applications. Secunia reckons a typical end-user PC with 50 programs installed will be faced with 3.5 times more security bugs in the 24 third-party programs running on their systems, than in the 26 Microsoft programs installed. Secunia expects this ratio to increase to 4.4 in 2010. Patching to defend against these vulnerabilities is further complicated by the 13 different software-update mechanisms running on each PC. Source: http://www.theregister.co.uk/2010/07/12/secunia_threat_report/

Stealthy, sophisticated technology threats are rampant. An overwhelming majority of companies have seen advanced security attacks on infrastructure, customer databases and internal systems by sophisticated malware, according to a report by the Ponemon Institute, an independent research and consulting firm dedicated to information management and privacy. The study, co-sponsored by the network-security vendor NetWitness, found 83 percent of 591 executives reported their companies have been targeted by advanced, stealthy attacks with more than 40 percent claiming they are targeted frequently. Other significant data from the study showed the that detecting threats was a time-consuming and accidental process rather than the result of proactive, information-technology management practices. Forty-six percent of companies took a month or longer to detect advanced threats; 45 percent discovered threats accidentally. Just over one-third (32 percent) believe they have adequate security technologies currently in place, with 26 percent reporting they have adequate security professionals working in their departments. Source: http://www.eweek.com/c/a/IT-Management/Stealthy-Sophisticated-Technology-Threats-Are-Rampant-898918/

National Monuments and Icons

(Arizona) **Forest crews hustle to protect burned hillsides.** Crews in the Schultz fire zone in Arizona continue to shore up burned hillsides with straw to combat possible floods and mudslides. Residents east of Flagstaff will continue to see helicopters dropping straw from the air July 16 and over the weekend. The aerial-protection efforts started on the northern end of the burn area and are working south. Coconino National Forest crews are scrambling to protect the fragile hillsides before monsoon thunderstorms roll into the charred area. Fifteen thousand acres burned last month due to an abandoned campfire. Investigators are still looking for the person or group that left the campfire in the Schultz Pass area. Source: http://www.kpho.com/news/24279111/detail.html

(California) **Two acid bombs found in Tilden Park parking lot.** Park rangers in Berkeley, California discovered two home-made acid bombs July 9 in the parking lot of the Tilden Regional Park. Officers from the East Bay Regional Parks Police and Fire arrived around 11:30 a.m., and confirmed the two suspicious devices were acid bombs — one-liter plastic bottles wrapped in duct tape containing acid and aluminum foil. The area was immediately evacuated and cordoned off. Contra Costa County hazardous materials specialists and members of the Walnut Creek Police Department's bomb squad attempted to detonate the two bombs, but the devices failed to explode. The two bombs were then

diffused and rendered safe. No suspects were arrested. East Bay Regional Parks police detectives will continue to investigate the incident. Source: http://www.mercurynews.com/ci_15487197

Postal and Shipping

(Wisconsin; Montana) **Man arrested in attempted bomb plot.** A 76-year-old Madison, Wisconsin, man was arrested July 12 in connection with an attempt to obtain an explosive device and send it to someone in Montana. A former Madison alderman and local attorney was arrested at his home in the 1600 block of Haas Street on suspicion of attempting to possess explosives. Police said the suspect's arrest follows an investigation that began after the suspect posted an ad on the Milwaukee section of the Craigslist Web site seeking someone to build him a bomb. Authorities said that they believe the suspect wanted to send the bomb to a Montana man who is a friend of the suspect's estranged wife. He wanted the bomb in a box and rigged to explode when it opened, according to authorities. The police report indicates that an agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives called the phone number in the ad and posed as a bomb maker. Authorities said the suspect offered to pay $500 for the bomb and described how he wanted it to work. Source: http://www.channel3000.com/news/24244224/detail.html

Public Health

Worker protection from pathogens said key in bioterror response. Adequate protections from airborne pathogens are crucial in protecting health workers and other responders from infection in the event of a disease outbreak or bio-terror attack, U.S. government researchers said July 14. A National Institute for Occupational Safety and Health senior researcher said the United States must have the ability to quickly boost the capacity of negative-pressure rooms — which prevent air from escaping into the wider environment or other similar quarantine areas. Only 60 percent of U.S. hospitals have structured units where airborne pathogens can be isolated. Their cost is usually between $30,000 and $40,000, the Center for Infectious Disease Research and Policy reported. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100715_7885.php

Hospital infection deaths caused by ignorance and neglect, survey finds. Deadly yet easily preventable bloodstream infections continue to plague American hospitals because facility administrators fail to commit resources and attention to the problem, according to a survey of medical professionals released July 12. An estimated 80,000 patients per year develop catheter-related bloodstream infections, or CRBSIs — which can occur when tubes that are inserted into a vein to monitor blood flow or deliver medication and nutrients are improperly prepared or left in longer than necessary. About 30,000 patients die as a result, according to the Centers for Disease Control and Prevention, accounting for nearly a third of annual deaths from hospital-acquired infections in the United States. Yet evidence suggests hospital workers could all but eliminate CRBSIs by following a five-step checklist that is stunningly basic: (1) Wash hands with soap; (2) clean patient's skin with an effective antiseptic; (3) put sterile drapes over the entire patient; (4) wear a sterile mask, hat, gown and gloves; (5) put a sterile dressing over the catheter site. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/07/12/AR2010071204893.html

(Missouri) **Whooping cough cases confirmed in Schuyler County.** The Missouri Department of Health and Senior Services is advising area residents of three confirmed cases of pertussis, or whooping

cough, in Schuyler County. According to a release, there are also 14 suspected cases in two Schuyler County Amish communities. The three people who took ill were hospitalized, and were all children, including a child less than 6 months old. The release stated that pertussis immunization coverage is low in the communities. There was also a recent outbreak with a Mennonite group in Morgan County. Pertussis is highly communicable and can cause severe disease or death in very young children. It begins with mild upper respiratory tract symptoms and progresses to a cough. The condition can further progress to severe paroxysms, often a characteristic inspiratory whoop followed by vomiting. Fever is absent or minimal. It can occur at any age, and should be considered in older children and adults who have a persistent cough lasting more than 7-14 days, which cannot be attributed to another specific illness, according to the release. Source: http://www.kirksvilledailyexpress.com/news/x1143361117/Whooping-cough-cases-confirmed-in-Schuyler-County

TRANSPORTATION

Stowaway's death in Airbus wheel well puts spotlight on Beirut security. Airport safety is getting a closer look in Lebanon after a body was discovered in the wheel well of a jet that took off from Beirut's airport. That incident occurred last week, when a 20-year-old man apparently sneaked onto the airport's runway and climbed into the wheel well of a Saudi Arabia-bound Airbus A320. The man died during the flight and his body was discovered by maintenance workers in Riyadh, according to The Daily Star of Lebanon. In the wake of the incident, The Associated Press reports "Lebanon's top security body has called for a 'comprehensive survey' of security measures at Beirut airport." The ill-fated stowaway appears to have used a metal cutter to cut through the barbed-wire fence surrounding the runway. In addition to the metal cutter, the Saudi Gazette writes "a cap and two cigarettes without filters were recovered from the tarmac, [the senior official] said, adding that the man appeared to have used the cigarette filters as ear plugs." A separate security official tells the publication that a family member of the victim said he suffered from mental illness. Source: http://travel.usatoday.com/flights/post/2010/07/stowaways-death-in-airbus-wheel-well-puts-spotlight-on-beirut-security/99963/1

(New Jersey) **Suspicious device found in car in Newark, NJ.** What appeared to be two gas cans connected by wires to a possible explosive device in Newark, New Jersey, turned out to be gas cans on a tool box, police said. Someone passing by noticed the cans in the back of a 1998 Dodge Omni parked near a railroad overpass that serves Amtrak and New Jersey Transit trains. Police blocked off a section of Oliver street so traffic could not go under the tracks, while they used a robot to examine the vehicle. Authorities used motor vehicle records to identify the car's owner as a 58-year-old man from Point Pleasant, New Jersey, and they are attempting to contact him. Source: http://abclocal.go.com/wabc/story?section=news/local&id=7554597

(California) **Police union says LAX vulnerable to terror attack.** Budget cuts have left Los Angeles International Airport vulnerable to a terrorist attack, according to the airport police union. In a letter obtained by Los Angeles radio station KNX, the Airport Peace Officers Association president said that security cutbacks have made the airport more vulnerable to terrorist attacks than at any time since September 11, 2001. He said the airport is particularly vulnerable to truck, car and luggage bombs. The officer said the airport police force is spread too thin in the central terminal area and random

checks of vehicles at the airport have been curtailed. The airport's executive director disputes the union allegations, saying the airport police budget has increased annually since the September 11 terrorist attacks. Source: http://www.ktla.com/news/landing/ktla-lax-security-terror-attack,0,5121549.story

(District of Columbia) **Driver of Metrobus had passengers fooled.** A 19-year-old man suspected of impersonating a Washington Metropolitan Area Transit Authority (Metro) bus driver July 9 and crashing a Route B2 bus carrying five adults and a baby before fleeing the scene initially drove so well that passengers thought he was a real Metro driver. The suspect was polite and knew the bus's exact route. The ride was business as usual until about 4:15 p.m. when the suspect hit a tree near 17th Street Southeast and Massachusetts Avenue in Washington D.C., about two blocks from the Stadium Armory Metro station. The suspect pried open the back doors, got off and then opened the front doors from the outside to let the six passengers off. He then got off the bus and took off running. Metro said July 10 it will review its procedures to determine how a non-Metro employee, who was wearing a Metro uniform, was able to board a bus and drive away without identifying himself or being challenged. A Metro spokeswoman said drivers are required to show identification upon arrival. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/07/11/AR2010071103460.html?wprss=rss_metro

Colton Harris-Moore captured in the Bahamas. A two-year, cross-country, international, multimillion-dollar crime spree ended with the July 11 arrest in the Bahamas of the notorious fugitive known as the "Barefoot Bandit." The fugitive is at risk of prosecution for more than 70 crimes across eight states, and in three countries. More than $3 million in stolen or ruined property is connected to him. Despite no flight training, no driver's license, no formal education for years and a tumultuous childhood, the teenager is suspected of piloting planes, stealing luxury cars, making off in pleasure boats and traveling from the Pacific Northwest to the Bahamas — all while wanted by authorities. He reportedly was seen running from police without shoes, which led to his headline-grabbing nickname. Police had to fire at the boat's engines to force him to stop. The suspect was taken by plane to Nassau, the island nation's capital, for processing. He is expected to appear in court there sometime this week. Source: http://www.heraldnet.com/article/20100712/NEWS01/707129947&news01ad=1

Water and Dams

(Texas; International) **Safety may be jeopardized as Rio Grande dams need repair.** The Rio Grande Valley in Texas remains possibly at risk after officials have not followed longstanding recommendations to shore up river dams along the U.S.-Mexico border. Records show that technical advisors to the International Boundary and Water Commission (IBWC) have recommended repairs at four dams along the Rio Grande from Donna to Del Rio, finding them to be from "marginally safe" to "potentially unsafe" — the second-worst safety action class officials give while evaluating dams. In one instance, a problem with sinkholes first noticed 20 years ago at Amistad Dam, near Mission, still continues. Concerns about regulating water flow at Retamal Dam, south of Donna, have persisted since 2005 and an issue with a sandbar was documented 13 years ago. Neither problem has been fixed. U.S. congressmen representing South Texas from Del Rio to Brownsville said they are closely monitoring developments. An IBWC spokeswoman stressed that inspectors believe the dams remain functional during flood conditions. The federally owned dams do not fall under Texas' responsibility

because they are not state-owned and are not private dams. Source: http://www.themonitor.com/articles/repair-40937-brownsville-rio.html

Waterborne diseases cost U.S. healthcare system more than $500 million annually. Research presented July 14 at the International Conference on Emerging Infectious Diseases indicated that hospitalizations for three, common water-borne diseases cost the U.S. health-care system as much as $539 million annually, according to a press release. Using data from a large insurance claims database between 2004 and 2007, a researcher at the Centers for Disease Control and Prevention and his colleagues estimated the hospitalization cost of three, common waterborne diseases in the United States: Legionnaires' disease, cryptosporidiosis and giardiasis. For each case of disease, they calculated the cost paid by the insurer, the out-of-pocket cost to the patient and the total amount paid. The release stated. "These cost data highlight that water-related diseases pose not only a physical burden to the thousands of people sickened by them each year, but also a substantial burden in health-care costs, including direct government payments through Medicare and Medicaid," he said. Source: http://watertechonline.com/news.asp?N_ID=74515

(Kentucky) **Chlorine gas leak prompts late-night panic.** A dangerous chlorine gas leak prompted evacuations, but some Lincoln County, Kentucky, families say the communication breakdown that followed may have caused more harm than the leak. The chlorine leak began at the Stanford water purification plant around 1 a.m. Officials said emergency management and haz-mat teams urged everyone within a 4-mile radius to evacuate, but some said they did not get the message. Emergency responders insist that was never a possibility, but many residents' fear was real when mixed signals led to confusion over whether their homes were affected. Police said chlorine levels were minimal, and they are convinced no one was ever in life-threatening danger. Police had begun knocking on doors within a 4-mile radius of the plant urging evacuations, but many neighbors just outside that radius said calls to 911 led them to believe they too were in danger. Now they say they are grateful no one was hurt in the process, but the incident shows a need for better communication in the future. Haz-mat crews contained the leak within about three hours. Stanford police said water plant officials are investigating what exactly caused the leak and how to prevent it from happening again. Source: http://www.wkyt.com/home/headlines/98720644.html

House approves overhaul of flood insurance program. Some subsidies would be ended and a measure of financial health would be restored under a House-approved overhaul of a program that provides flood insurance to more than 5 million homeowners and businesses in flood-prone areas. The legislation, which approves operations of the National Flood Insurance Program for five years, also allows for some premium and deductible increases as the program tries to recover from Katrina and other 2005 hurricanes that left it some $18.75 billion in debt to the U.S. Treasury. The measure passed 329-90 on Thursday. The flood program, an arm of the Federal Emergency Management Agency (FEMA), has for more than four decades offered affordable insurance to more than 20,000 communities that participate in flood damage reduction efforts and to residents in federally designated flood zones. It was created in 1968 because of the reluctance of private insurers to cover flood damage. Congress has not updated the program since 1994. In the ensuing years the once-solvent program had to pay out some $17 billion in Katrina-related claims and had to deal with FEMA flood zone remapping that has thrust thousands of homes and businesses into areas where they are required to buy flood insurance. The legislation now goes to the Senate, where its fate is uncertain.

Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/07/15/AR2010071504312_pf.html

(Pennsylvania) **Police: Group climbed Dover Twp. tower, had access to water supply.** Northern York County Regional Police arrested four people — three male juveniles and a man — June 23 after they scaled the top of a Dover Township, Pennsylvania water tower and opened the roof cover. The late-night trespassing, at Carlisle Road and Skytop Trail, warranted an investigation by Dover Township Public Works officials and the state department of environmental protection, police said July 13. "Nothing that we know of was put into the water supply or put into the tower itself," a police lieutenant said. Police charged the three York County juveniles, one who is 19, and two others who are either 16 or 17, of the 4800 block of Ziegler's Church Road in Spring Grove, with criminal conspiracy, possession of instruments of crime, criminal trespass and disorderly conduct. Police also included a request for restitution to cover the cost of the emergency response by Dover Township Public Works Department employees. Police responded to the tower after a call from a resident. The tower, which is maintained by the township, was designed to hold more than 1 million gallons of water, police said. The group used a wrench to remove a barrier from the access ladder. Once on the roof, they took off the cover that would have allowed access to the water supply, police said. Source: http://www.ydr.com/crime/ci_15508081

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**